

1 Jennifer Lynch (SBN 240701)
jlynch@eff.org
2 Hanni M. Fakhoury (SBN 252629)
hanni@eff.org
3 ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
4 San Francisco, CA 94109
Telephone: (415) 436-9333
5 Facsimile: (415) 436-9993
6 Counsel for *Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION
7
8

9 UNITED STATES DISTRICT COURT
10 FOR THE NORTHERN DISTRICT OF CALIFORNIA
11 SAN JOSE DIVISION
12

13) Case No.: 5:15-xr-90304-HRL (LHK)
14)
15) IN RE APPLICATION FOR TELEPHONE) **BRIEF *AMICUS CURIAE* OF**
16) INFORMATION NEEDED FOR A CRIMINAL) **ELECTRONIC FRONTIER**
17) INVESTIGATION) **FOUNDATION IN SUPPORT OF A**
18)) **WARRANT REQUIREMENT FOR**
19)) **HISTORICAL CELL SITE**
20) **INFORMATION**
21)
22)
23)
24)
25)
26)
27)
28)

TABLE OF CONTENTS

INTRODUCTION	1
ARGUMENT	2
I. AMERICANS HAVE A SUBJECTIVE EXPECTATION OF PRIVACY IN LOCATION INFORMATION.....	2
A. Research Shows Americans Believe the Data on and Generated by their Cell Phones is Private.....	2
B. Courts Recognize the Privacy Implications of Location Information.....	3
II. AN EXPECTATION OF PRIVACY IN CELL PHONE DATA IS OBJECTIVELY REASONABLE EVEN THOUGH THE DATA IS HELD BY A PHONE COMPANY.	5
III. THE NATIONWIDE TREND TOWARD GREATER PROTECTION FOR PRIVACY IN PHONE RECORDS AND LOCATION INFORMATION SHOWS SOCIETY RECOGNIZES THAT A PRIVACY INTEREST IN THIS DATA IS REASONABLE.	9
CONCLUSION	13

TABLE OF AUTHORITIES

Federal Cases

<i>Arizona v. Evans</i> , 514 U.S. 1 (1995)	1
<i>Bond v. United States</i> , 529 U.S. 334 (2000)	2
<i>Doe v. Broderick</i> , 225 F.3d 440 (4th Cir. 2000)	10
<i>In re Application of U.S. for Historical Cell Site Data</i> , 724 F.3d 600 (5th Cir. 2013)	5
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	1, 12
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	1
<i>Oliver v. United States</i> , 466 U.S. 170 (1984)	2, 10
<i>Oregon Prescription Drug Monitoring Program v. DEA</i> , 998 F. Supp. 2d 957 (D. Or. 2014)	7
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	1, 4, 6, 13
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	<i>passim</i>
<i>United States v. Cooper</i> , 2015 WL 881578 (N.D. Cal. Mar. 2, 2015)	1, 10
<i>United States v. Cotterman</i> , 709 F.3d 952 (9th Cir. 2013) (en banc)	6
<i>United States v. Davis</i> , 2015 WL 2058977 (11th Cir. 2015) (en banc)	5
<i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004)	6
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012)	4, 7, 11, 12

1	<i>United States v. Lopez</i> ,	12
	895 F. Supp. 2d 592 (D. Del. 2012)	
2	<i>United States v. Maynard</i> ,	10
3	615 F.3d 544 (D.C. Cir. 2010).....	
4	<i>United States v. Nerber</i> ,	10
5	222 F.3d 597 (9th Cir. 2000)	
6	<i>United States v. Powell</i> ,	12
	943 F. Supp. 2d 759 (E.D. Mich. 2013)	
7	<i>United States v. Robinson</i> ,	6
8	414 U.S. 218 (1973)	
9	<i>United States v. Velasquez</i> ,	10
10	2010 WL 4286276 (N.D. Cal. Oct. 22, 2010)	
11	<i>United States v. Warshak</i> ,	7
	631 F.3d 266 (6th Cir. 2010)	
12	<i>Virginia v. Moore</i> ,	10
13	553 U.S. 164 (2008)	
14	State Cases	
15	<i>Commonwealth v. Augustine</i> ,	<i>passim</i>
16	4 N.E.3d 846 (Mass. 2014).....	
17	<i>Commonwealth v. Melilli</i> ,	11
	555 A.2d 1254 (Pa. 1989).....	
18	<i>Commonwealth v. Rousseau</i> ,	12
19	990 N.E.2d 543 (Mass. 2013).....	
20	<i>Commonwealth v. Rushing</i> ,	12
21	71 A.3d 939 (Pa. Sup. Ct. 2013), <i>overruled on other grounds</i> 99 A.3d 416 (2014)	
22	<i>Ellis v. State</i> ,	11
	353 S.E.2d 19 (Ga. 1987)	
23	<i>People v. Blair</i> ,	8, 9, 11
24	25 Cal. 3d 640 (1979).....	
25	<i>People v. Chapman</i> ,	8
26	36 Cal. 3d 98 (1984)	
27	<i>People v. DeLaire</i> ,	11
	610 N.E.2d 1277 (Ill. Ct. App. 1993)	

1	<i>People v. McKunes</i> ,	
	51 Cal. App. 3d 487 (1975)	8
2	<i>People v. Palmer</i> ,	
3	24 Cal. 4th 856 (2001)	8
4	<i>People v. Sporleder</i> ,	
5	666 P.2d 135 (Colo. 1983)	11
6	<i>People v. Weaver</i> ,	
	909 N.E.2d 1195 (N.Y. 2009)	11
7	<i>State v. Brereton</i> ,	
8	826 N.W.2d 369 (Wis. 2013)	12
9	<i>State v. Campbell</i> ,	
10	759 P.2d 1040 (Or. 1988)	11
11	<i>State v. Earls</i> ,	
	70 A.3d 630 (N.J. 2013)	5, 7, 12
12	<i>State v. Gunwall</i> ,	
13	720 P.2d 808 (Wash. 1986)	11
14	<i>State v. Hunt</i> ,	
15	450 A.2d 952 (N.J. 1982)	11
16	<i>State v. Jackson</i> ,	
	76 P.3d 217 (Wash. 2003)	11
17	<i>State v. Rothman</i> ,	
18	779 P.2d 1 (Haw. 1989)	11
19	<i>State v. Shaktman</i> ,	
20	553 So.2d 148 (Fla. 1989)	11
21	<i>State v. Thompson</i> ,	
	760 P.2d 1162 (Id. 1988)	11
22	<i>State v. Zahn</i> ,	
23	812 N.W.2d 490 (S.D. 2012)	12
24	<i>Tracey v. State</i> ,	
	152 So. 3d 504 (Fla. 2014)	5, 8, 12

Federal Statutes

26	18 U.S.C. § 3122	8, 9
27	18 U.S.C. § 3123	9

1	18 U.S.C. § 3124	9
2	18 U.S.C. § 3125	9
3	18 U.S.C. § 3126	9
4	18 U.S.C. § 3127	9

State Statutes

6	16 Maine Rev. Stat. Ann. § 648	12
7	18 Pa. Cons. Stat. Ann. § 5761	11
8	725 ILCS 168/10	12
9	Colo. Rev. Stat. Ann. § 16-3-303.5	12
10	Haw. Rev. Stat. § 803-44.7.....	11
11	Ind. Code § 35-33-5-12	12
12	Md. Code, Criminal Procedure 1-203.1	12
13	Minn. Stat. Ann. §§ 626A.28	12
14	Mont. Code Ann. § 46-5-110	12
15	Okla. Stat. Ann. tit. 13, § 177.6.....	11
16	Or. Rev. Stat. § 165.663	11
17	Or. Rev. Stat. Ann. § 133.619	11
18	S.C. Code Ann. § 17-30-140	11
19	Utah Code Ann. § 77-23c-102.....	12
20	Va. Code Ann. 19.2-56.2.....	12
21	Wis. Stat. Ann. § 968.373.....	12

State Rules

24	69 Ops. Cal. Atty. Gen 55 (1986).....	9
25	86 Ops. Cal. Atty. Gen. 198 (2003).....	9

Federal Constitutional Provisions

U.S. Const. amend. IV	<i>passim</i>
-----------------------------	---------------

State Constitutional Provisions

Cal. Const. art. I, § 13.....	8
-------------------------------	---

Other Authorities

David Deasy, <i>TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size</i> , TRUSTe Blog (Sept. 5, 2013).....	3
Jan Lauren Boyles et al., <i>Privacy and Data Management on Mobile Devices</i> , Pew Research Internet & American Life Project (Sept. 5, 2012)	3
Janice Y. Tsai et al., <i>Location-Sharing Technologies: Privacy Risks and Controls</i> , Carnegie Mellon University (Feb. 2010)	3
Kathryn Zickuhr, <i>Location-Based Services</i> , Pew Research Internet and American Life Project (Sept. 12, 2013)	3
Lee Rainie, <i>Cell Phone Ownership Hits 91% of Adults</i> , Pew Research Center (June 6, 2013).....	2
Pew Research Center, <i>Public Perceptions of Privacy and Security in the Post-Snowden Era</i> (Nov. 12, 2014).....	3
Stephen E. Henderson, <i>Learning From all Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search</i> , 55 Cath. U. L. Rev. 373 (2006)	11
Steven Shepard, <i>Americans Continue to Drop Their Landline Phones</i> , National Journal (Dec. 18, 2013).....	2
United States Census Bureau, <i>Quick Facts</i>	11

INTRODUCTION

“With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.” *Arizona v. Evans*, 514 U.S. 1, 17-18 (1995) (O’Connor, J., concurring). In the 35 years since the Supreme Court decided *Smith v. Maryland*, 442 U.S. 735 (1979), the capacity for technology to reveal unexpectedly detailed information about our lives has increased exponentially. Where, in *Smith*, the government recorded the numbers dialed and received on one phone at one location for three days, today the government can obtain not just those numbers but also all the locations the phone’s owner traveled while the phone was able to make or receive a call. This technology was “nearly inconceivable just a few decades ago.” *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). As the Supreme Court recognized in *Kyllo v. United States*, given advances in technology, courts must increasingly address “what limits there are upon this power of technology to shrink the realm of guaranteed privacy.” 533 U.S. 27, 34 (2001).

Courts and legislatures across the country are responding to changing technologies by pushing beyond the case law of 36 years ago and enacting greater privacy protections for the data—including location information—we store on our devices, in the “cloud,” and with third parties. As more Americans have a subjective expectation of privacy in their location data, these expectations necessarily become ones that “society is prepared to recognize [are] ‘reasonable,’” and thus protected by the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Judge Lloyd’s decision below recognized this reality, adopting Judge Illston’s opinion in *United States v. Cooper*, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) (unpublished) and concluding that “cell site location information implicates a person’s constitutional right to privacy.” Order at 4, Dkt. No. 2 (April 9, 2015). This Court should affirm Judge Lloyd’s decision and require the government use a probable cause search warrant to obtain historical cell site location information.

ARGUMENT

I. AMERICANS HAVE A SUBJECTIVE EXPECTATION OF PRIVACY IN LOCATION INFORMATION.

Owning a cell phone is not a luxury; today more than 90%¹ of all American adults have a cell phone, and landline phones are becoming increasingly obsolete.² Cell phones generate a staggering amount of data about where the phone’s owner has travelled throughout her daily life, including through cell site location information (“CSLI”). Society is increasingly recognizing that location data like this deserves “the most scrupulous protection from government invasion.” *Oliver v. United States*, 466 U.S. 170, 178 (1984) (citation omitted).

Many federal and state courts have recognized an expectation of privacy in location and phone records generally and CSLI specifically. As more people live in states where these records are deemed private—including California—the government cannot assert it is unreasonable to expect privacy in them. Thus, Judge Lloyd was correct to require a probable cause search warrant to obtain CSLI.

A. Research Shows Americans Believe the Data on and Generated by their Cell Phones is Private.

For the Fourth Amendment to apply, a person must “exhibit[] an actual expectation of privacy.” *Bond v. United States*, 529 U.S. 334, 338 (2000). Recent studies show Americans expect privacy in the data stored on and generated by their cell phones, including location information. Within the last year, the Pew Research Center reported that 82% of Americans consider the details of their physical location over time to be sensitive information—more sensitive

¹ Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, Pew Research Center (June 6, 2013), <http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/>.

² See Steven Shepard, *Americans Continue to Drop Their Landline Phones*, National Journal (Dec. 18, 2013), <http://www.nationaljournal.com/hotline-on-call/americans-continue-to-drop-their-landline-phones-20131218> (citing CDC statistics finding 36.5% of U.S. adults live in household with no landline phone).

than their relationship history, religious or political views, or the content of their text messages.³ In 2012, the Pew Center found that cell phone owners take a number of steps to protect access to their personal information and mobile data, and more than half of phone owners with mobile apps have uninstalled or decided to not install an app due to concerns about the privacy in their personal information.⁴ In addition, more than 30% of smart phone owners polled took affirmative steps to safeguard their privacy: 19% turned off location tracking on their phones and 32% cleared their browsing or search history.⁵ The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned location services off.⁶ A 2013 survey conducted on behalf of the Internet company TRUSTe found 69% of American smart phone users did not like the idea of being tracked.⁷ And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that participants believed the risks of location-sharing technologies outweighed the benefits and were “extremely concerned” about controlling access to their location information.⁸

B. Courts Recognize the Privacy Implications of Location Information.

Given these statistics, it is unsurprising that courts around the country have also recognized

³ Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 34, 36-37 (Nov. 12, 2014),

http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (50% of respondents believed location information was “very sensitive.”).

⁴ Jan Lauren Boyles et al., *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012), <http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/>.

⁵ *Id.*

⁶ Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet and American Life Project (Sept. 12, 2013), <http://www.pewinternet.org/2013/09/12/location-based-services/>.

⁷ David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013), <http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/>.

⁸ Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University 12 (Feb. 2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

the privacy implications of location information. In 2012, the Supreme Court suggested in *United States v. Jones* that people expect their otherwise public movements on the street to remain private. 132 S. Ct. 945 (2012). Although the Court ultimately held that placing a GPS tracking device on a car was a “search” because it was a physical trespass onto private property, in two separate concurring opinions, five members of the Supreme Court recognized that location tracking could violate a reasonable expectation of privacy. Justice Sotomayor questioned “whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on.” *Id.* at 956 (Sotomayor, J., concurring). And Justice Alito wrote on behalf of three other justices, “society’s expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual’s car for a very long period.” *Id.* at 964 (Alito, J., concurring).⁹

In the wake of *Jones*, several state and federal courts have recognized the privacy implications of location information and historical CSLI specifically. In protecting cell site data in *Commonwealth v. Augustine*, the Massachusetts Supreme Judicial Court recognized that this data may raise even greater privacy concerns than GPS tracking devices placed on a car because cell site data can track “the user’s location far beyond the limitations of where a car can travel”—including into “constitutionally protected areas” like a home. 4 N.E.3d 846, 861-62 (Mass. 2014). *Augustine* also noted historical cell site data gave police access to something it would never have with traditional law enforcement investigative methods: the ability “to track and reconstruct a

⁹ The Supreme Court in *Riley v. California* specifically cited Justice Sotomayor’s concurring opinion in *Jones* as a reason to limit police searches of cell phones incident to arrest. 134 S. Ct. at 2490. *Riley* recognized the privacy implications of location information, noting that cell phones store data that can “reveal where a person has been,” making it possible to “reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.” *Id.* (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

person's past movements." *Id.* at 865. Similarly, in *State v. Earls*, the New Jersey Supreme Court noted users should be "entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives" and adopted a warrant requirement for historical CSLI. 70 A.3d 630, 644 (N.J. 2013). And the Florida Supreme Court in *Tracey v. State* noted "the close relationship an owner shares with his cell phone" makes "a cell phone's movements its owner's movements." 152 So. 3d 504, 525 (Fla. 2014). The court concluded there was a subjective expectation of privacy "in the location signals transmitted solely to enable the private and personal use of his cell phone, even on public roads." *Id.*

II. AN EXPECTATION OF PRIVACY IN CELL PHONE DATA IS OBJECTIVELY REASONABLE EVEN THOUGH THE DATA IS HELD BY A PHONE COMPANY.

This subjective expectation of privacy in CSLI is not defeated simply because this location information is exposed to the telephone company. The government has consistently relied on the Supreme Court's opinion in *Smith v. Maryland*, 442 U.S. 735—ruling there was no expectation of privacy in the phone numbers a person dials—to argue that today's cell phone users have no expectation of privacy in historical CSLI because that data has been exposed to a third party. *See, e.g.* Appeal of Denial of Application for Telephone Information Needed for a Criminal Investigation ("Gov. Appeal") at 4, Dkt. No. 4 (April 30, 2015); *see also United States v. Davis*, 2015 WL 2058977, at *11-12 (11th Cir. 2015) (en banc) (finding no expectation of privacy in CSLI under *Smith*); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 612-13 (5th Cir. 2013) (same). According to the government, when a person voluntarily uses a cell phone, she knows the phone is sending information about her location to the phone company and thus cannot expect the phone company to keep that information private. *See* Gov. Appeal at 5, Dkt. No. 4. But *Smith* does not alter the calculus here for two reasons.

1 First, the data here is significantly more revealing than the limited three days' worth of call
2 records at issue in *Smith*. The Supreme Court in *Riley v. California* recognized that cell phones
3 store "qualitatively different" types of data compared to physical records and noted that because
4 today's advanced technology can disclose much more revealing personal information than
5 technologies of the past, the "scope of the privacy interests at stake" far exceed that of any
6 analogue in the physical world. 134 S. Ct. at 2490-91. Although, the government argued in *Riley*
7 that cellphones are "materially indistinguishable" from physical items that may be searched
8 without a warrant incident to arrest like the pack of cigarettes at issue in *United States v. Robinson*,
9 414 U.S. 218, 236 (1973), the Court refused to equate the two. *Riley*, 134 S. Ct. at 2488-89. It
10 believed comparing a search of all data on a cell phone to the search of physical items is "like
11 saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways
12 of getting from point A to point B, but little else justifies lumping them together." *Riley*, 134 S.
13 Ct. at 2488.

14
15 Similarly, here, because the data generated by CSLI is so different in quantity and quality
16 from the data generated by a simple landline phone, this Court cannot rely only on antiquated cases
17 to determine how to protect cell phone data, especially data that reveals sensitive location
18 information. *Id.* at 2488-89. Even before *Riley*, the Ninth Circuit adopted a similar approach in
19 *United States v. Cotterman* when it ruled that the government's ability to conduct suspicionless
20 searches at the international border did not extend to the forensic examination of a computer. 709
21 F.3d 952, 968 (9th Cir. 2013) (en banc). Noting that "technology matters," the Court explained
22 that digital information "stands in stark contrast to the generic and impersonal contents of a gas
23 tank." *Id.* at 964 (referring to *United States v. Flores-Montano*, 541 U.S. 149, 155 (2004)
24 (permitting suspicionless dismantling and inspection of a car's gas tank)). Following *Riley* and
25 *Cotterman*, this Court should adopt the same approach, taking CSLI for what it is—data that paints
26
27
28

1 a rich and revealing portrait of an individual’s life, movements and associations—rather than
2 relying on cases involving distinguishable—and primitive—technologies and less invasive
3 government action.

4 Second, *Smith* does not reflect the realities of modern society. Today we share much more
5 information about ourselves with third parties merely as a byproduct of the differences in how we
6 perform tasks today versus in the past—whether it is writing emails instead of letters; collaborating
7 on document drafting online instead of through hard-copy printouts, or buying and reading books
8 on our phones or Kindles versus purchasing a physical book at a bookstore to read later in the
9 privacy of our own homes. As Justice Sotomayor noted in *Jones*, *Smith*’s basic “premise” is “ill
10 suited to the digital age, in which people reveal a great deal of information about themselves to
11 third parties in the course of carrying out mundane tasks.” 132 S. Ct. at 957 (Sotomayor, J.,
12 concurring). Homing in on subjective expectations of privacy, Justice Sotomayor doubted “people
13 would accept without complaint the warrantless disclosure” of information to the government like
14 URLs they visit or the phone numbers they dial or text. *Id.*

15 Other courts have reached the same conclusions, both before and after *Jones*, finding
16 expectations of privacy in data stored by third parties, including emails stored on a service
17 provider’s servers, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); patient prescription
18 records stored in an online database, *Oregon Prescription Drug Monitoring Program v. DEA*, 998
19 F. Supp. 2d 957 (D. Or. 2014), *appeal docketed*, No. 14-35402; and even CSLI itself. *See, e.g.,*
20 *Augustine*, 4 N.E.3d at 850; *Earls*, 70 A.3d at 644. As the Florida Supreme Court noted in finding
21 an expectation of privacy in real-time CSLI notwithstanding *Smith*, cell phones are so
22 “indispensable” that “cell phone tracking can easily invade the right to privacy in one’s home or
23
24
25
26
27
28

1 other private areas.” *Tracey*, 152 So. 3d at 524.¹⁰ *Tracey* noted a person did not “voluntarily
 2 convey that information to the service provider for any purpose other than to enable use of his cell
 3 phone for its intended purpose” and rejected the “fiction” that people consent to warrantless cell
 4 phone tracking as a condition of carrying a cell phone. *Id.* at 523-25.

5 Third, *Smith* not only fails to capture the technology at issue here, it has also been rejected
 6 by the California Supreme Court. Just months after *Smith* was decided, the state high court ruled in
 7 *People v. Blair* that Californians have an expectation of privacy in their phone records under
 8 Article I, Section 13 of the state constitution, the state equivalent to the Fourth Amendment.
 9 25 Cal. 3d 640, 655 (1979).¹¹ While *Smith* held phone customers have no subjective expectation of
 10 privacy in dialed phone numbers because they “convey” the numbers to the company to have the
 11 calls connected, 442 U.S. at 742, *Blair* instead focused on the fact that a list of telephone calls
 12 provides a “virtual current biography” of a person. 25 Cal. 3d at 653. Since it was “virtually
 13 impossible for an individual” to “function in the modern economy without a telephone,” these
 14 records were not voluntarily disclosed. *Id.* Thus, police need a warrant to obtain the records under
 15 the state constitution. *Id.* at 655; *see also People v. Chapman*, 36 Cal. 3d 98, 106-111 (1984),
 16 disapproved on other grounds in *People v. Palmer*, 24 Cal. 4th 856 (2001) (expectation of privacy
 17 in unlisted telephone number); *People v. McKunes*, 51 Cal. App. 3d 487, 492 (1975) (expectation
 18 of privacy in telephone company’s customer records).¹²
 19
 20
 21

22 ¹⁰ The Court’s analysis in *Tracey* was solely under the Fourth Amendment. *See* 152 So. 3d at 511-
 23 12.

24 ¹¹ Article 1, section 13 of the California constitution states in whole “The right of the people to be
 25 secure in their persons, houses, papers, and effects against unreasonable seizures and searches may
 26 not be violated; and a warrant may not issue except on probable cause, supported by oath or
 27 affirmation, particularly describing the place to be searched and the persons and things to be
 28 seized.”

¹² The California Attorney General has issued two opinions making clear that state law
 enforcement personnel must obtain a search warrant to install and use a pen register. First, in 1986,

For this reason, the government’s argument that cell phone users—especially those within this Court’s jurisdiction in Northern California—cannot expect location information to remain private once the data has been exposed to the phone company is incorrect. On the contrary, all Californians have been promised that, because cell phone data reveals detailed personal information, cell phone customers have a reasonable expectation of privacy in that data, even though it is held by a third party. *Blair*, 25 Cal. 3d at 653.

Ultimately, that means *Smith* does not control the outcome of this case. Just because technology is *capable* of disclosing what is otherwise private information about a person’s specific location does not mean that a person has a lesser expectation of privacy under the Fourth Amendment.

III. THE NATIONWIDE TREND TOWARD GREATER PROTECTION FOR PRIVACY IN PHONE RECORDS AND LOCATION INFORMATION SHOWS SOCIETY RECOGNIZES THAT A PRIVACY INTEREST IN THIS DATA IS REASONABLE.

Having established that people generally have a subjective expectation of privacy in their location, that advances in technology require changes in legal analyses, and that Californians specifically have an expectation of privacy in phone records, the question remains whether broader society is prepared to recognize that subjective expectation of privacy as reasonable. The answer is

the Attorney General clarified that although California has no statutes governing pen registers, state magistrates were authorized to issue a search warrant supported by probable cause to permit police to install and use them. *See* 69 Ops. Cal. Atty. Gen 55 (1986). Later that year, Congress passed a set of federal statutes governing the installation and use of pen registers. *See* 18 U.S.C. §§ 3122-3127. Congress required state and federal law enforcement to obtain judicial authorization to install and use a pen register but only required the government to demonstrate the evidence obtained via pen register is “relevant to an ongoing criminal investigation” rather than require probable cause. 18 U.S.C. §§ 3122(a)(2), (b)(2). For state law enforcement, the use of the federal pen register statute has to be consistent with state law. 18 U.S.C. § 3122(a)(2). So in 2003, the state Attorney General clarified that since *Blair* placed the information obtained from a pen register—a list of phone numbers dialed—within the “zone of privacy protected by the state Constitution,” state law enforcement could not rely on federal law to install a pen register. 86 Ops. Cal. Atty. Gen. 198 at *3-4 (2003).

yes. As Judge Illston noted in *Cooper*, “[s]ociety’s expectation of privacy in historical cell site data is also evidenced by many state statutes and cases which suggest this information exists within the ambit of an individual’s personal and private realm.” *Cooper*, 2015 WL 881578, at *8.

A court reviewing the appropriate Fourth Amendment limits to be placed on searches must necessarily look to “societal understandings” of what should be considered private to determine reasonable expectations of privacy. *Oliver*, 466 U.S. at 178. Further, while the Fourth Amendment is not “a redundant guarantee of whatever limits on search and seizure legislatures might have enacted,” *Virginia v. Moore*, 553 U.S. 164, 168 (2008), the existence of both federal and state statutory protection for certain kinds of information helps inform whether society has determined that a particular expectation of privacy is reasonable. *See, e.g., United States v. Maynard*, 615 F.3d 544, 564 (D.C. Cir. 2010) (“state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable”); *Doe v. Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (federal statutory protection “is relevant to the determination of whether there is a ‘societal understanding’” of a legitimate expectation of privacy in medical records); *United States v. Nerber*, 222 F.3d 597, 604-05 (9th Cir. 2000) (federal wiretap statute is “strong evidence” that society would find warrantless video surveillance unreasonable); *see also Cooper*, 2015 WL 881578, at *8 (“While state law is, of course, not dispositive on this question, ‘the recognition of a privacy right by numerous states may provide insight into broad societal expectations of privacy.’”) (quoting *United States v. Velasquez*, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010)).

The societal recognition of privacy in phone records and location information is reflected in federal and state cases and state statutes deeming this data to be private. After *Smith* was decided, courts in California, Colorado, Hawaii, Idaho, Illinois, New Jersey, Pennsylvania, Washington and Florida all rejected *Smith*, finding those states’ residents had a reasonable expectation of privacy

under their state constitutions in dialed phone numbers—notwithstanding the fact those records are held by the phone provider.¹³ By statute, Georgia and Oregon required police to demonstrate probable cause to install and operate a pen register to obtain dialed phone numbers.¹⁴

Then, as technology continued to advance but before *Jones* was decided, the state supreme courts of New York, Oregon, and Washington held that people could reasonably expect privacy in their location, meaning that using technology to track a person’s movements was a Fourth Amendment “search.”¹⁵ Five state legislatures passed statutes requiring police to obtain a probable cause search warrant to track a person’s location with a tracking device like a GPS—even when the person is traveling in public places.¹⁶ This meant that even before the Supreme Court addressed the question of whether Americans have a reasonable expectation of privacy in their location information, seven states—representing nearly 20% of the United States population¹⁷—already recognized this privacy right.

After *Jones*, the number of people across the country reasonably expecting privacy in their location has increased, as more courts have recognized that an expectation of privacy in a person’s

¹³ See *People v. Blair*, 602 P.2d 738, 746 (Cal. 1979); *People v. Sporleder*, 666 P.2d 135, 141-43 (Colo. 1983); *State v. Rothman*, 779 P.2d 1, 7-8 (Haw. 1989); *State v. Thompson*, 760 P.2d 1162, 1165-67 (Id. 1988); *People v. DeLaire*, 610 N.E.2d 1277, 1282 (Ill. Ct. App. 1993); *State v. Hunt*, 450 A.2d 952, 955-57 (N.J. 1982); *Commonwealth v. Melilli*, 555 A.2d 1254, 1256-59 (Pa. 1989); *State v. Gunwall*, 720 P.2d 808, 813-17 (Wash. 1986); *State v. Shaktman*, 553 So.2d 148 (Fla. 1989); see generally Stephen E. Henderson, *Learning From all Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

¹⁴ See *Ellis v. State*, 353 S.E.2d 19, 21-22 (Ga. 1987) (pen register is “device” under Ga. Code Ann. § 16-11-64(b) whose installation requires probable cause search warrant); Or. Rev. Stat. § 165.663.

¹⁵ See, e.g., *People v. Weaver*, 909 N.E.2d 1195, 1201 (N.Y. 2009) (GPS); *State v. Campbell*, 759 P.2d 1040, 1048-49 (Or. 1988) (use of radio transmitter to locate automobile); *State v. Jackson*, 76 P.3d 217, 223-24 (Wash. 2003) (GPS).

¹⁶ See Haw. Rev. Stat. § 803-44.7(b); Okla. Stat. Ann. tit. 13, § 177.6(A); Or. Rev. Stat. Ann. § 133.619(6); 18 Pa. Cons. Stat. Ann. § 5761(c)(4); S.C. Code Ann. § 17-30-140(b)(2).

¹⁷ This figure is based on 2013 population data for each state, as projected by the U.S. Census. See United States Census Bureau, *Quick Facts*, <http://quickfacts.census.gov/qfd/index.html> (last visited June 11, 2015).

location means technologies like GPS or real-time cell phone tracking are Fourth Amendment “searches” under *Katz*.¹⁸

Courts and state legislatures have also extended privacy protections to CSLI. The high courts in Florida, Massachusetts and New Jersey—relying in part on Justice Sotomayor’s concurrence in *Jones*—recognized a reasonable expectation of privacy in CSLI under their respective state constitutions and required police use a search warrant to obtain that information. *Tracey*, 152 So.3d at 526; *Augustine*, 4 N.E.3d at 850; *Earls*, 70 A.3d at 644. Five more states legislated privacy protections for historical cell site data, with Colorado, Maine, Minnesota, Montana and Utah passing statutes expressly requiring law enforcement to apply for a search warrant to obtain this data.¹⁹

In sum, the number of people in the United States—and in California specifically—who have been promised by court decision or legislation that information about where they have been is private has never been higher. The growing number of people protected by the warrant requirement, while not dispositive of whether there is a Fourth Amendment expectation of privacy in historical CSLI, is compelling proof of “societal understandings” as to what level of privacy and security is reasonable. Thus Judge Lloyd’s decision should be affirmed.

¹⁸ *Commonwealth v. Rousseau*, 990 N.E.2d 543, 552-53 (Mass. 2013) (GPS); *Commonwealth v. Rushing*, 71 A.3d 939, 961-64 (Pa. Sup. Ct. 2013), *overruled on other grounds* 99 A.3d 416 (2014) (cell phone signal); *State v. Brereton*, 826 N.W.2d 369, 379 (Wis. 2013) (GPS); *United States v. Powell*, 943 F. Supp. 2d 759, 776-77 (E.D. Mich. 2013) (real time cell site tracking); *State v. Zahn*, 812 N.W.2d 490, 496-499 (S.D. 2012) (GPS); *United States v. Lopez*, 895 F. Supp. 2d 592, 602 (D. Del. 2012) (GPS).

¹⁹ See Colo. Rev. Stat. Ann. § 16-3-303.5(2); 16 Maine Rev. Stat. Ann. § 648; Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a). Six states have passed laws requiring police obtain a search warrant to track a cell phone in real time. See, Ind. Code § 35-33-5-12; Wis. Stat. Ann. § 968.373(2); 725 ILCS 168/10; Md. Code, Criminal Procedure 1-203.1; Va. Code Ann. 19.2-56.2; HB 1440 which amended Wash. Rev. Code 9.73.260 on May 11, 2015.

CONCLUSION

For more than 90% of Americans, a cell phone is the only phone they have. As anyone who moves about in society recognizes, cell phones are constantly in use in both public and private spaces. At the same time, they are also “constantly connecting to cell sites, and those connections are recorded” by cell phone companies. *Augustine*, 4 N.E.3d at 860. This means that Americans are constantly generating an almost unfathomable wealth of information about their whereabouts.

When it comes to historical cell site records, it is clear that Americans generally and Californians specifically expect that the location information revealed by these records remain private. Given the trend in courts and legislatures across the country to protect this privacy interest by requiring a warrant, society understands this expectation of privacy is reasonable.

This Court should follow the Supreme Court’s lead in *Riley v. California* and recognize that, given the vast amount of data generated by cell phones, coupled with the trend toward greater privacy protections for that data, outdated cases cannot govern the outcome here. Americans have a reasonable expectation of privacy in the location data generated by CSLI, and, as the Court noted in *Riley*, the answer to the question of what police must do before they may obtain that data is “simple—get a warrant.” 134 S. Ct. at 2495.

DATED: June 12, 2015

Respectfully submitted,

By: Hanni M. Fakhoury

Hanni M. Fakhoury

Jennifer A. Lynch

ELECTRONIC FRONTIER FOUNDATION

815 Eddy Street

San Francisco, CA 94109

Telephone: (415) 436-9333

Facsimile: (415) 436-9993

Counsel for *Amicus Curiae*

ELECTRONIC FRONTIER FOUNDATION